Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Wayne
Last Name: Workman
Mailing Address: 1480 Mundy Dr.
City: Florissant
Country: United States
State or Province: MO
ZIP/Postal Code: 63031
Email Address: wayne.workman2012@gmail.com
Organization Name:
Comment: I am developing a specialized capture portal for flashable router/access points. This specialized software is to promote businesses to share their WiFi with customers and generate revenue from sharing.

The wifi is ad-based, requiring a user to watch an ad to use the guest WiFi, and every 30 minutes thereafter. This will generate revenue for businesses that already share free wifi with customers, and will lower the cost of businesses sharing wifi, therefore promoting free and open WiFi to the general public, and drawing in more customers for said businesses.

If the proposed rule by the FCC is implemented, this will destroy my business plans, it will destroy the potential for a business to easily generate revenue by sharing WiFi. It will destroy the low-entry-cost that I plan to make available to all businesses everywhere for free.

Do not pass this rule. It will inhibit technological advancements, stunt potential business models, slow the adoption of free WiFi among businesses, and raise the cost of a business implementing free guest WiFi.

This proposed rule is a terrible rule - and it will destroy all the work I've conducted in my private time over the past several months.

There are many, many other very valid and important reasons why this proposed rule is terrible, but these reasons listed here are what's most important to me.

I am developing a specialized capture portal for flashable router/access points. This specialized software is to promote businesses to share their WiFi with customers and generate revenue from sharing.

The wifi is ad-based, requiring a user to watch an ad to use the guest WiFi, and every 30 minutes thereafter. This will generate revenue for businesses that already share free wifi with customers, and will lower the cost of businesses sharing wifi, therefore promoting free and open WiFi to the general public, and drawing in more customers for said businesses.

If the proposed rule by the FCC is implemented, this will destroy my business plans, it will destroy the potential for a business to easily generate revenue by sharing WiFi. It will destroy the low-entry-cost that I plan to make available to all businesses everywhere for free.

Do not pass this rule. It will inhibit technological advancements, stunt potential business models, slow the adoption of free WiFi among businesses, and raise the cost of a business implementing free guest WiFi.

This proposed rule is a terrible rule - and it will destroy all the work I've conducted in my private time over the past several months.

There are many, many other very valid and important reasons why this proposed rule is terrible, but these reasons listed here are what's most important to me.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Matt
Last Name: Morgan
Mailing Address: 804 W 180th St. #41
City: New York
Country: United States
State or Province: NY
ZIP/Postal Code: 10033
Email Address: matt@concretecomputing.com
Organization Name:
Comment: Greetings. My name is Matt Morgan; I'm a resident of New York City where I've worked in technology for nonprofit organizations for over 20 years. Among my proudest achievements is jumpstarting the availability of free, public Wifi in the city in 2004, when Brooklyn Museum--where I ran the IT department--set up what was, and may remain, the largest free public wifi hotspot in the city, for very low cost. Since then, millions of Brooklyn Museum visitors have benefited--because the same infrastructure that provided free Internet access to all comers also served to deliver network connections to the Museum's in-gallery technology.

It may not surprise you to hear that we built that system on open source software, such as OpenWRT, NoCat, and WifiDog. There was no commercial software on any router at the time that would have made our work feasible for the budget that was available, and the innovation that came out of those efforts is still paying off today. So it surprised me to hear that you've proposed new rules that would prevent that sort of experimentation, innovation, and growth.

I respect your desire to manage usage of the common radio spectrum. But I ask you not to approve these new rules as proposed.

First, the regulations on software defined radios should not restrict the ability to replace software on computing devices.

As written, the regulations require that manufacturers prevent modification of all software computing devices which use software defined radios. The Commission should amend the regulations in a manner which protects the traditional right of law-abiding users to understand and improve the software on their own devices.

Second, the regulations on e-labels should not restrict the ability to replace software on computing devices.

The signers appreciate the need for proper labeling of wireless devices and the requirements set by Congress in the E-Label Act. The Commission should amend the regulations to guarantee electronic labels do not interfere with the ability of downstream parties to install any software they so choose.

Thank you for your attention.

All my best,
Matt Morgan

Greetings. My name is Matt Morgan; I'm a resident of New York City where I've worked in technology for nonprofit organizations for over 20 years. Among my proudest achievements is jumpstarting the availability of free, public Wifi in the city in 2004, when Brooklyn Museum--where I ran the IT department--set up what was, and may

remain, the largest free public wifi hotspot in the city, for very low cost. Since then, millions of Brooklyn Museum visitors have benefited--because the same infrastructure that provided free Internet access to all comers also served to deliver network connections to the Museum's in-gallery technology.

It may not surprise you to hear that we built that system on open source software, such as OpenWRT, NoCat, and WifiDog. There was no commercial software on any router at the time that would have made our work feasible for the budget that was available, and the innovation that came out of those efforts is still paying off today. So it surprised me to hear that you've proposed new rules that would prevent that sort of experimentation, innovation, and growth.

I respect your desire to manage usage of the common radio spectrum. But I ask you not to approve these new rules as proposed.

First, the regulations on software defined radios should not restrict the ability to replace software on computing devices.

As written, the regulations require that manufacturers prevent modification of all software computing devices which use software defined radios. The Commission should amend the regulations in a manner which protects the traditional right of law-abiding users to understand and improve the software on their own devices.

Second, the regulations on e-labels should not restrict the ability to replace software on computing devices.

The signers appreciate the need for proper labeling of wireless devices and the requirements set by Congress in the E-Label Act. The Commission should amend the regulations to guarantee electronic labels do not interfere with the ability of downstream parties to install any software they so choose.

Thank you for your attention.

All my best,
Matt Morgan

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Joseph
Last Name: Loo
Mailing Address: 28152 Driver ave #3
City: Agoura Hills
Country: United States
State or Province: CA
ZIP/Postal Code: 91301
Email Address: jloo@acm.org
Organization Name:
Comment: The proposal rules is too open ended. It indicates that people who want to use wifi and not the standard windows will not be able to install their operating system

The proposal rules is too open ended. It indicates that people who want to use wifi and not the standard windows will not be able to install their operating system

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Lowell
Last Name: Sochia
Mailing Address: 6814 SE Jack Rd
City: Milwaukie
Country: United States
State or Province: OR
ZIP/Postal Code: 97222
Email Address: lhsochia@gmail.com
Organization Name:
Comment: I am opposed to not allowing the consumer who purchased a product to not be able to modify it. What kind of country is this? And why do we the people have to keep fighting for their rights, this country is becoming a joke.

This ruling is violating our rights as Americans, and should not be allowed to be passed. Who is the idiot who thought this one up???

I am opposed to not allowing the consumer who purchased a product to not be able to modify it. What kind of country is this? And why do we the people have to keep fighting for their rights, this country is becoming a joke.

This ruling is violating our rights as Americans, and should not be allowed to be passed. Who is the idiot who thought this one up???

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Kevin
Last Name: Fowler
Mailing Address: 739 Sandlewood Drive
City: Canal Fulton
Country: United States
State or Province: OH
ZIP/Postal Code: 44614
Email Address:
Organization Name:
Comment: Wireless networking research depends on the ability of researchers to investigate and modify their devices. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. Not fixing security holes either feeds cyberthreats or increases electronic waste. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing. In short please allow us to continue to control our own computing devices by not passing this proposed rule.

Wireless networking research depends on the ability of researchers to investigate and modify their devices. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. Not fixing security holes either feeds cyberthreats or increases electronic waste. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing. In short please allow us to continue to control our own computing devices by not passing this proposed rule.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: christopher
Last Name: raday
Mailing Address: 13838 s springfield ave
City: crestwood
Country: United States
State or Province: IL
ZIP/Postal Code: 60445
Email Address:
Organization Name:
Comment: I would like to voice my opinion against the topic of limiting a device owners use of thier own devices.
I can see that you have good intention in creating this rule, but the inintended consequences are great. By restriciting a users ability to operate thier device as they see it, sets a precedent that a user may only run what code the government gives them. This would be stiffeling toward progress in all of computer science.
Alos, the recent scandal involving VolksWagon using thier embeded code to cheat emmisions regulations should highlight the fact that more openness is needed and not allow anyone to hide, obscure, or restrict thier code.

I would like to voice my opinion against the topic of limiting a device owners use of thier own devices.
I can see that you have good intention in creating this rule, but the inintended consequences are great. By restriciting a users ability to operate thier device as they see it, sets a precedent that a user may only run what code the government gives them. This would be stiffeling toward progress in all of computer science.
Alos, the recent scandal involving VolksWagon using thier embeded code to cheat emmisions regulations should highlight the fact that more openness is needed and not allow anyone to hide, obscure, or restrict thier code.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Darren
Last Name: Weber
Mailing Address: POB 1333
City: Winchester
Country: United States
State or Province: VA
ZIP/Postal Code: 22604
Email Address: AdvantageFirst@gmail.com
Organization Name: Advantage Investigation & Protection, LLC
Comment: It is very important to allow end users to install software of their choice on all forms of hardware platforms. Not only does it support a wide range of after market businesses, It allows the user to correct firmware security issues.

Any legal measures implemented should protect open source software, which is an important element to ensure integrity and competition throughout the software industry.

It is very important to allow end users to install software of their choice on all forms of hardware platforms. Not only does it support a wide range of after market businesses, It allows the user to correct firmware security issues.

Any legal measures implemented should protect open source software, which is an important element to ensure integrity and competition throughout the software industry.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Anonymous
Last Name: Anonymous
Mailing Address: 1527 Brewster
City: Indianapolis
Country: United States
State or Province: IN
ZIP/Postal Code: 46260
Email Address: support@hartcoblogsite.org
Organization Name: null
Comment: Please don't implement this. I Install my own operating system on many of my devices.to threaten my lively hood is to threaten me.

Please don't implement this. I Install my own operating system on many of my devices.to threaten my lively hood is to threaten me.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Sam
Last Name: Jensen
Mailing Address: 1100 E. Acacia Ave
City: El Segundo
Country: United States
State or Province: CA
ZIP/Postal Code: 90245
Email Address:
Organization Name:
Comment: These rules are ill-advised. Please do not implement them.

It's all but certain these rules are intended to preclude unlicensed operators from illegally modifying part 15 equipment to increase their range.

On the surface, these rules seem like a good thing, however, an unintended consequence will be to preclude rapid deployment of patches to close security holes in the manufacturers' firmware.

Very few days go by without news of some seemingly impenetrable company (or even government agency) having their security breached. These breaches could have serious consequences for many people - even those that are not trying to administer their own network.

These rules seemingly aid and abet those persons that are up to no good.

These rules will foreclose one more tool that security conscious individuals might employ to slow down the loss of the data they are trying to protect.
Why not enforce the rules you have in place right now?

Router manufacturers are not likely to preclude access to the radio and still allow the rest of the router to be modified. They are far more likely to preclude all access to their hardware's operation.

These rules are ill-advised. Please do not implement them.

These rules are ill-advised. Please do not implement them.

It's all but certain these rules are intended to preclude unlicensed operators from illegally modifying part 15 equipment to increase their range.

On the surface, these rules seem like a good thing, however, an unintended consequence will be to preclude rapid deployment of patches to close security holes in the manufacturers' firmware.

Very few days go by without news of some seemingly impenetrable company (or even government agency) having their security breached. These breaches could have serious consequences for many people - even those that are not trying to administer their own network.

These rules seemingly aid and abet those persons that are up to no good.

These rules will foreclose one more tool that security conscious individuals might

employ to slow down the loss of the data they are trying to protect.
Why not enforce the rules you have in place right now?

Router manufacturers are not likely to preclude access to the radio and still allow the rest of the router to be modified. They are far more likely to preclude all access to their hardware's operation.

These rules are ill-advised. Please do not implement them.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Loc
Last Name: BERNARD
Mailing Address: 64 rue d'amour
City: vignacourt
Country: France
State or Province: somme
ZIP/Postal Code: 80650
Email Address: null
Organization Name: null
Comment: I am respectfully asking the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

Wireless networking research depends on the ability of researchers to investigate and modify their devices.
Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
Not fixing security holes either feeds cyberthreats and increases electronic waste.
Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

I am respectfully asking the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

Wireless networking research depends on the ability of researchers to investigate and modify their devices.
Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
Not fixing security holes either feeds cyberthreats and increases electronic waste.
Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Loc
Last Name: BERNARD
Mailing Address: 64 rue d'amour
City: vignacourt
Country: France
State or Province: somme
ZIP/Postal Code: 80650
Email Address: null
Organization Name: null
Comment: I am respectfully asking the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

Wireless networking research depends on the ability of researchers to investigate and modify their devices.
Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
Not fixing security holes either feeds cyberthreats and increases electronic waste.
Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

I am respectfully asking the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

Wireless networking research depends on the ability of researchers to investigate and modify their devices.
Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
Not fixing security holes either feeds cyberthreats and increases electronic waste.
Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Tom
Last Name: Kocourek
Mailing Address: 396 Laurel Trace
City: Carrollton
Country: United States
State or Province: GA
ZIP/Postal Code: 30116
Email Address:
Organization Name: N4FWD - licensed US Amateur Radio operator
Comment: As pointed out by numerous commenters, if someone wishes to abuse the rules and regulations governing Part 15 RF router devices (wireless routers), locking down the firmware will not prevent this abuse.

These Part 15 devices (wireless routers) form the basis for a Part 97 device with a firmware update. By blocking modification of the firmware of Part 15 devices, the FCC rulemaking would also block legitimate use of these devices as a Part 97 device. (http://www.aredn.org/) (http://www.broadband-hamnet.org/)

A legitimate alternative would be enforcement of existing Part 15 rules and regulations and levee fines on those who would abuse the Part 15 rules and regulations.

As pointed out by numerous commenters, if someone wishes to abuse the rules and regulations governing Part 15 RF router devices (wireless routers), locking down the firmware will not prevent this abuse.

These Part 15 devices (wireless routers) form the basis for a Part 97 device with a firmware update. By blocking modification of the firmware of Part 15 devices, the FCC rulemaking would also block legitimate use of these devices as a Part 97 device. (http://www.aredn.org/) (http://www.broadband-hamnet.org/)

A legitimate alternative would be enforcement of existing Part 15 rules and regulations and levee fines on those who would abuse the Part 15 rules and regulations.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: David
Last Name: McCortney
Mailing Address: 890 Tallmadge Rd
City: Kent
Country: United States
State or Province: OH
ZIP/Postal Code: 44240
Email Address: dmccortn@cs.kent.edu
Organization Name:
Comment: Please do not prevent people from modifying embedded software on hardware they own. There are already ways to detect unlawful broadcasting, and these approaches are more than sufficient to protect the public from unlawful wireless signals. Digital rights management on WiFi is better described as an unnecessary restriction. Companies that want DRM may use new laws to help obtain and keep a monopoly. Projects such as LibreWRT respect the freedom of users and are also economical, if they are legislated out of existence then no one wins. The public will no longer be free to modify WiFi devices and will turn to older technologies such as wires and manually copying files on physical media. The companies that benefit over the short term will diminish over the long term. Criminals will find other ways to illegally change WiFi using hardware modifications. The danger of interrupting emergency broadcasts is very real, yet there is no real benefit to preventing the installation of competing operating systems. Rather such restriction will have a chilling effect on innovation and prevent legitimate uses, such as running GNU/Linux on a router.

Please do not prevent people from modifying embedded software on hardware they own. There are already ways to detect unlawful broadcasting, and these approaches are more than sufficient to protect the public from unlawful wireless signals. Digital rights management on WiFi is better described as an unnecessary restriction. Companies that want DRM may use new laws to help obtain and keep a monopoly. Projects such as LibreWRT respect the freedom of users and are also economical, if they are legislated out of existence then no one wins. The public will no longer be free to modify WiFi devices and will turn to older technologies such as wires and manually copying files on physical media. The companies that benefit over the short term will diminish over the long term. Criminals will find other ways to illegally change WiFi using hardware modifications. The danger of interrupting emergency broadcasts is very real, yet there is no real benefit to preventing the installation of competing operating systems. Rather such restriction will have a chilling effect on innovation and prevent legitimate uses, such as running GNU/Linux on a router.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Ralph
Last Name: Bromley
Mailing Address: 1300 Renshaw Road
City: Chester
Country: United States
State or Province: PA
ZIP/Postal Code: 19013
Email Address: dancingmadrb3@gmail.com
Organization Name:
Comment: I use linux as my primary operating system, for the FCC to impose a rule forcing routers not to use linux as a backend is a stupid idea and reeks of Microsoft offering money to the FCC.
Open source firmware is a necessary evil as it allows routers to be easier to work with for all operating systems and not just the FCC's boss Microsoft.
But I guess they only want windows and .exe's as they cannot understand that windows is adware, syware, virtus infected crap.
This is typical, a big government organization trying to kill linux innoivation because they sleep in Bill Gates mansion

I use linux as my primary operating system, for the FCC to impose a rule forcing routers not to use linux as a backend is a stupid idea and reeks of Microsoft offering money to the FCC.
Open source firmware is a necessary evil as it allows routers to be easier to work with for all operating systems and not just the FCC's boss Microsoft.
But I guess they only want windows and .exe's as they cannot understand that windows is adware, syware, virtus infected crap.
This is typical, a big government organization trying to kill linux innoivation because they sleep in Bill Gates mansion

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Kent
Last Name: Adams
Mailing Address: 13207 West Lake Road #14
City: Vermilion
Country: United States
State or Province: OH
ZIP/Postal Code: 44089
Email Address: InstructorAdams@gmail.com
Organization Name:
Comment: I would like to voice my opposition the proposed rules in FCC 15-92. These rules require manufacturers to demonstrate that they have restricted the ability of the consumer/end-user to modify the wireless components of devices they have purchased. While these rules may be well intentioned to protect from unwanted signal interference, they do a great disservice to open source software developers, contributors, and users.

Working in the technology industry, I am happy to be able to modify my devices and ensure they are compatible with the way my product operates regardless of what an end user may do or how a technology may change. Having access to open source firmware modules allows me to craft scenarios which provide for very specific and/or very general outcomes similar to what a user may experience from around the world.

By hampering an end-user's ability to modify the device you will be stymieing innovation, allowing security vulnerabilities to go untested and unchecked, and doing a disservice to legitimate commerce activities.

I would like to voice my opposition the proposed rules in FCC 15-92. These rules require manufacturers to demonstrate that they have restricted the ability of the consumer/end-user to modify the wireless components of devices they have purchased. While these rules may be well intentioned to protect from unwanted signal interference, they do a great disservice to open source software developers, contributors, and users.

Working in the technology industry, I am happy to be able to modify my devices and ensure they are compatible with the way my product operates regardless of what an end user may do or how a technology may change. Having access to open source firmware modules allows me to craft scenarios which provide for very specific and/or very general outcomes similar to what a user may experience from around the world.

By hampering an end-user's ability to modify the device you will be stymieing innovation, allowing security vulnerabilities to go untested and unchecked, and doing a disservice to legitimate commerce activities.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Travis
Last Name: Bretton
Mailing Address: 2588 E. Woods End Ct.
City: Boise
Country: United States
State or Province: ID
ZIP/Postal Code: 83706
Email Address:
Organization Name:
Comment: To Whom it May Concern,

I am a software engineer. I have been in this position through 21 years and 9 industries. I have worked on mainframes all the way down to portable devices. I mention this so that you may understand that my perspective on this proposed rule comes from a career spent in the thick of the changes that have radically changed the technology in this country.

The proposal to force the conformity and verification of devices with RF radios will stifle the creativity and innovation that has created the very technology you're proposing to regulate.

Much of the research and advances in this country are achieved on computers that run Linux, a free and open source operating system that most likely was not verified by the manufacturer. If these computers also have an RF radio then the manufacturer will block any operating system that they do not control and benefit from.

The effort to make our systems more secure and safe is done by researchers who aren't afraid to customize devices in order to find security flaws. It certainly isn't going to be done by manufacturers not interested in spending more capital to fix the vulnerabilities in their devices. And make no mistake--the very people and activities this proposed rule is intended to target--criminals and digital terrorists--aren't going to follow these rules.

Please, while the goal of the proposed rule is laudable, it needs revising with an eye towards how this rule will affect the law abiding people in this country who don't do things in the strictly normal way; the people who like to tinker; the people who push the boundaries of what their hardware can do. You know--the people responsible for most technological innovations.

To Whom it May Concern,

I am a software engineer. I have been in this position through 21 years and 9 industries. I have worked on mainframes all the way down to portable devices. I mention this so that you may understand that my perspective on this proposed rule comes from a career spent in the thick of the changes that have radically changed the technology in this country.

The proposal to force the conformity and verification of devices with RF radios will stifle the creativity and innovation that has created the very technology you're proposing to regulate.

Much of the research and advances in this country are achieved on computers that run Linux, a free and open source operating system that most likely was not verified by

the manufacturer. If these computers also have an RF radio then the manufacturer will block any operating system that they do not control and benefit from.

The effort to make our systems more secure and safe is done by researchers who aren't afraid to customize devices in order to find security flaws. It certainly isn't going to be done by manufacturers not interested in spending more capital to fix the vulnerabilities in their devices. And make no mistake--the very people and activities this proposed rule is intended to target--criminals and digital terrorists--aren't going to follow these rules.

Please, while the goal of the proposed rule is laudable, it needs revising with an eye towards how this rule will affect the law abiding people in this country who don't do things in the strictly normal way; the people who like to tinker; the people who push the boundaries of what their hardware can do. You know--the people responsible for most technological innovations.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Jason
Last Name: Charles
Mailing Address: 5916 Wallace Rd
City: Panama City
Country: United States
State or Province: FL
ZIP/Postal Code: 32404
Email Address: jasontcharles@gmail.com
Organization Name:
Comment: To whom it may concern,

I respectfully ask you to consider NOT making any changes that would restrict the modification of software or firmware in a electronic wireless device by parties other than the manufacturer. Any move to restrict the modification would severely impact the security and integrity of wireless devices. I will give you a firm and irrefutable example in the consumer grade router market. A large community has formed around the modification of consumer grade wireless routers that overcomes the limitations and security posture of most wireless routers on the market. Tomato, DD-WRT, OpenWRT, Broadband-Hamnet to name a few that were aimed to make routers more configurable and more secure. I for one use the "TomatoUSB" firmware on a Netgear router. This has allowed me to more finely tune my network and implement advanced security that I would not otherwise be able to do.

Another such example is the major advancements that has occurred in the SDR (Software Defined Radio) space. Very inexpensive radio dongles have been used to experiment with various passive listening methods and modes. My concern is that any rules change will stifle such advancements for both the hardware manufacturer and the experimenter that uses this technology. Most all of the technology has been used for very productive benign activities such as the massive ADS-B network that has been formed to keep track of aircraft and send the data to an aggregate like Flightware. I have personally used this to keep track of family member's flights and am thankful that so many can contribute to the network. All this is possible with the modification of a simple SDR receiver.

I sincerely hope that any changes you make to the rules will encourage the responsible modification and use by third parties and not restrict changes to only the manufacturer. This will certainly stifle any progress that is being made in those device spaces.

Sincerely,
Jason Charles

To whom it may concern,

I respectfully ask you to consider NOT making any changes that would restrict the modification of software or firmware in a electronic wireless device by parties other than the manufacturer. Any move to restrict the modification would severely impact the security and integrity of wireless devices. I will give you a firm and irrefutable example in the consumer grade router market. A large community has formed around the modification of consumer grade wireless routers that overcomes the limitations and security posture of most wireless routers on the market. Tomato, DD-WRT, OpenWRT, Broadband-Hamnet to name a few that were aimed to make routers more

configurable and more secure. I for one use the "TomatoUSB" firmware on a Netgear router. This has allowed me to more finely tune my network and implement advanced security that I would not otherwise be able to do.

Another such example is the major advancements that has occurred in the SDR (Software Defined Radio) space. Very inexpensive radio dongles have been used to experiment with various passive listening methods and modes. My concern is that any rules change will stifle such advancements for both the hardware manufacturer and the experimenter that uses this technology. Most all of the technology has been used for very productive benign activities such as the massive ADS-B network that has been formed to keep track of aircraft and send the data to an aggregate like Flightware. I have personally used this to keep track of family member's flights and am thankful that so many can contribute to the network. All this is possible with the modification of a simple SDR receiver.

I sincerely hope that any changes you make to the rules will encourage the responsible modification and use by third parties and not restrict changes to only the manufacturer. This will certainly stifle any progress that is being made in those device spaces.

Sincerely,
Jason Charles

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: Hctor Graco
Last Name: Cavalcanti Saavedra
Mailing Address: Route du Condroz 107
City: Lige
Country: Belgium
State or Province: Lige
ZIP/Postal Code: 4031
Email Address:
Organization Name:
Comment: As a young student in Computer Science, I find it important for users to have the freedom to run the software of their choice in their own devices, because:
* Wireless networking research depends on the ability of researchers to investigate and modify their devices.
* Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
* Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
* Not fixing security holes either feeds cyberthreats or increases electronic waste.
* Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.
Furthermore, as jailbreaking is considered legal, so should flashing custom firmware on devices with a modular wireless radio or with an electronic label. More freedom guarantees faster scientific development and economic growth.

I hope you will take these points in consideration and do not implement rules that take away the ability of users to install the software of their choice on their computing devices.

As a young student in Computer Science, I find it important for users to have the freedom to run the software of their choice in their own devices, because:
* Wireless networking research depends on the ability of researchers to investigate and modify their devices.
* Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
* Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
* Not fixing security holes either feeds cyberthreats or increases electronic waste.
* Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.
Furthermore, as jailbreaking is considered legal, so should flashing custom firmware on devices with a modular wireless radio or with an electronic label. More freedom guarantees faster scientific development and economic growth.

I hope you will take these points in consideration and do not implement rules that take away the ability of users to install the software of their choice on their computing devices.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations
FR Document Number: 2015-21634
RIN:
Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:
First Name: John
Last Name: Brooks
Mailing Address: 691 Island Park Drive
City: Ottawa
Country: Canada
State or Province: Ontario
ZIP/Postal Code: K1Y 0B8
Email Address:
Organization Name:
Comment: Please do not implement rules that ban end-user low-level software modification of wireless-capable consumer devices. Your concern about harmful emissions potentially caused by consumer devices is not unreasonable, but this is absolutely the wrong way to go about preventing it.

Many thousands of people use open-source or alternative operating systems and firmware on their devices. The ability to do this not only allows users the freedom of choice in the software they use, but it also allows users and developers to extend and improve functionality on those devices.

By banning such modifications, you are stifling both freedom and innovation and putting users at the mercy of vendors with profit interests. Vendors can and do often choose to drop support for older hardware, meaning that security and functionality issues go unresolved in the official software. In these cases, actively developed open source/alternative software is a key part of keeping devices secure and up-to-date.

Such rules would also harm amateur radio operators and technicians, as they would no longer be able to invent, test, and create new ways of wireless networking using consumer hardware. Distributed, decentralized mesh networks would be made impossible as the amateurs who operate these would no longer be able to do so.

End users, developers, amateur radio technicians, inventors, and researchers need you to do what is right, not simply what is easy. A bad decision like the one proposed would carry an enormous economical and environmental (e-waste) cost. Please do not implement these rules.

Please do not implement rules that ban end-user low-level software modification of wireless-capable consumer devices. Your concern about harmful emissions potentially caused by consumer devices is not unreasonable, but this is absolutely the wrong way to go about preventing it.

Many thousands of people use open-source or alternative operating systems and firmware on their devices. The ability to do this not only allows users the freedom of choice in the software they use, but it also allows users and developers to extend and improve functionality on those devices.

By banning such modifications, you are stifling both freedom and innovation and putting users at the mercy of vendors with profit interests. Vendors can and do often choose to drop support for older hardware, meaning that security and functionality issues go unresolved in the official software. In these cases, actively developed open source/alternative software is a key part of keeping devices secure and up-to-date.

Such rules would also harm amateur radio operators and technicians, as they would no longer be able to invent, test, and create new ways of wireless networking using consumer hardware. Distributed, decentralized mesh networks would be made impossible as the amateurs who operate these would no longer be able to do so.

End users, developers, amateur radio technicians, inventors, and researchers need you to do what is right, not simply what is easy. A bad decision like the one proposed would carry an enormous economical and environmental (e-waste) cost. Please do not implement these rules.